Maryland Cybersecurity Coordinating Council

Thursday, April 15, 2021
9:00 AM - 10:00 AM

Call to Order: Chip Stewart: 9:01am

Roll Call:

<table>
<thead>
<tr>
<th>Council Member</th>
<th>Title</th>
<th>Organization</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Charles “Chip” Stewart</td>
<td>SCISO &amp; Chairman</td>
<td>DoIT</td>
<td>Present</td>
</tr>
<tr>
<td>Walter “Pete” Landon</td>
<td>Director</td>
<td>GoHS</td>
<td>Represented by Mark Hubbard</td>
</tr>
<tr>
<td>David Brinkley</td>
<td>Secretary</td>
<td>DBM</td>
<td>Represented by Derek Mitchell</td>
</tr>
<tr>
<td>Ellington Churchill</td>
<td>Secretary</td>
<td>DGS</td>
<td>Represented by Eric Lomboy</td>
</tr>
<tr>
<td>Lourdes Padilla</td>
<td>Secretary</td>
<td>DHS</td>
<td>Represented by Jitendra Chandra</td>
</tr>
<tr>
<td>Robert Green</td>
<td>Secretary</td>
<td>DPSCS</td>
<td>Represented by Stanley Lofton</td>
</tr>
<tr>
<td>Dennis Schrader</td>
<td>Secretary</td>
<td>MDH</td>
<td>Represented by Matthew Otwell</td>
</tr>
<tr>
<td>Timothy Gowen</td>
<td>Adjutant General</td>
<td>DMIL</td>
<td>Represented by Brig. Gen. Adam Flasch</td>
</tr>
<tr>
<td>Russell Strickland</td>
<td>Director</td>
<td>MEMA</td>
<td>Present</td>
</tr>
<tr>
<td>Woodrow Jones</td>
<td>Superintendent</td>
<td>MSP</td>
<td>Represented by Maj. Tawn Gregory</td>
</tr>
<tr>
<td>Gregory Slater</td>
<td>Secretary</td>
<td>MDOT</td>
<td>Represented by Ken Hlavacek</td>
</tr>
</tbody>
</table>

Vote to Approve Meeting Minutes from January 28, 2021, 9:03am

Moved - Russell Strickland, MEMA
Second - Major Tawn Gregory, MSP

Stewart: Is there any debate or discussion?

Stewart: Are there any who are opposed to approving the meeting minutes from January 28, 2021? If so, please say “Nay.”

Nay-0
Unfinished Business

A. ATO/SSP Subcommittee Laura Gomez-Martin, DoIT

March 2021 - First ATO subcommittee meeting occurred. Findings from the initial committee meeting revealed that most agencies do follow an ATO process, but the vision for the upcoming months is to establish a common procedure that all agencies will follow. Additionally, templates and draft documents were reviewed at this meeting.

April 2021 - Creation is the key focus for the month of April; the committee will be open to new proposals. This month, we will consider when an ATO is necessary (E.g., will an ATO occur for critical systems only? Will legacy systems undergo the ATO process?).

May 2021 - May will focus on reviewing documentation and presenting the documents to Maryland Cybersecurity Coordinating Council (“MCCC”) council members.

June 2021 - In June, the goal is to consider and incorporate any feedback received.

July 2021 - The RFP Subcommittee will launch in July 2021. Any interest from the MCCC council members should be communicated in an email to Laura Gomez-Martin.

New Business

A. Presentation: Legislative Update Chip Stewart, DoIT

<table>
<thead>
<tr>
<th>Bill</th>
<th>Title</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SB0049/HB0038</td>
<td>State Government - Department of Information Technology - Cybersecurity</td>
<td>Passed Senate with minor Amendments Passed House with minor Amendments</td>
</tr>
<tr>
<td>SB0348</td>
<td>State Government – Information Technology – Cybersecurity</td>
<td>Key provisions integrated into SB69 Voted down in Senate</td>
</tr>
<tr>
<td>SB0351</td>
<td>State Government – Protection of Information – Revisions (Maryland Data Privacy Act)</td>
<td>Passed Senate Stalled in House Committee</td>
</tr>
<tr>
<td>SB0917/HB0587</td>
<td>Department of Information Technology - Status of Information Technology and Cybersecurity in State and Local Agencies</td>
<td>Stalled in House/Senate Committees. Some provisions integrated into SB69</td>
</tr>
<tr>
<td>SB0069/HB0879</td>
<td>Cybersecurity Coordination and Operations - Establishment and Reporting</td>
<td>Passed Senate &amp; House with significant Amendments Stalled in conference committee</td>
</tr>
</tbody>
</table>
SB0049- Passed, includes definition of cybersecurity strategy, and guidance for municipalities, subdivisions, schools. This is a guidance, not mandatory, but does compel DoIT to oversee and advise cybersecurity matters for all state agencies and higher education.

SB0231- Stewart expects to see this next year-this pertains to security awareness and training.

SB0069--Mentions of resources used to recover from cybersecurity events. If this passes (next year), classification and reporting requirements could be created. This will be based on NIST 800-61.

B. Presentation: Third Party Vendor Breach, Ken Hlavacek, MDoT

Objective: Provide information to viewers with information on how to respond in the event of a security breach.

Average breach can take ¼ of a year to detect.

**What to do at discovery?** Gather information. If a vendor has been breached, research the data that may be accessible through your account. What systems could be compromised in your environment that the vendor has connections to?

When a breach has been discovered, a Cyber Report Form (located on the DoIT website) must be completed and submitted to DoIT. Updates may also need to be provided as the investigation on the data breach continues. The form requests the following information:

- Point of Contact (POCs)
- What happened
- What data is exposed (is it public data/private data)

**How to prepare for a breach?**

- Use NIST as a guide and final Standard Operating Procedure (SOP)--ensure this SOP includes a strong communication plan and review the SOPs with the vendor
- Establish procedures with the vendor, prior to a breach
- Engage in tabletop exercises

**Scenario One:** Division of a company was compromised. Agency not informed for about a month and a half. The vendor conceals the breach, but news eventually leaks. The agency discovers the breach through the media. The division impacted does not impact your agency.

- Agency reviews network connections with vendor (shuts down some connections)
- Agency establishes daily calls

**Scenario Two:** Vendor notifies State agency immediately and provides POCs. Daily calls are established.
Scenario Three: Large vendor company, small breach within vendor organization that does not impact State network but there is a State data relationship. Agency is notified of the breach via snail mail. Vendor provides a timeline of actions and remediation for the incident. Agency engages Incident Response (IR) team and works through SOPs.

- Be mindful that vendors will not have the same policies/process for notifying customers

Lofton: Who should be in a tabletop exercise?
Hlavacek: The tabletop exercise would include IT, up to leadership, and in some cases the vendor would participate as well.

Lofton: Is the [Cyber Report Form] sent each time there is an update?
Stewart: The form is completed once and DoIT works with the agency moving forward to gather updates.

Chandna inquired as to whether the incident response procedure would be a good addition to the ATO subcommittee. Stewart believes it would be a good topic of discussion to add.

C. Presentation: State Cybersecurity Insurance Chip Stewart, DoIT

Average cost of breach exceeding $8 million.

The State Treasurer’s Office is responsible for cybersecurity insurance (response costs, recovery cost, fines, replacement). If one of the state agencies has interest in learning more, please contact STO or Chip Stewart

Reporting is important, and all incidents (small and large alike) should be reported in a timely manner. If we do not report to the insurance company in a timely manner, we may lose coverage.

Open Discussion, Council Members/Desigees

No discussion

Adjournment: Chip Stewart, 9:36am

Motion- Major Gregory
Second- Chandra Jitendra

All those not in favor of adjourning the Maryland Cybersecurity Coordinating Council please say “Nay.” Nay-0

Nay- 0

Charles Stewart (Jul 23, 2021 09:17 EDT) Date: Jul 23, 2021